Eric Luiijf *(eric.luiijf@tno.nl)*,
André Smulders *(andre.smulders@tno.nl)*,
Pauline Kamphuis *(thehaguesecuritydelta.com)*

Kanttekeningen bij de Europese cyber security strategie

In februari presenteerde de Europese Unie de Europese cyber security strategie en begeleidende concept richtlijn. The Hague Security Delta (HSD) is verheugd dat de Nederlandse Nationale Cyber Security Strategie nu ook op Europees niveau navolging krijgt. Toch plaatsen we een paar kanttekeningen.

Foto: Europese Commissie

Publiekprivate Samenwerking (PPS)

HSD onderschrijft het belang van publiek-private samenwerking, die de EU voor het bevorderen van internetveiligheid wil stimuleren. Als groeiend netwerk van bedrijven, overheden en kennisinstituten in de Nederlandse veiligheidssector is HSD een goed voorbeeld van “de gouden driehoek”. We maken ons samen sterk voor innovatieve veiligheidsoplossingen en economische ontwikkeling. De Europese strategie beschrijft verantwoordelijkheden voor regelgevende instanties en overheden, als internetgebruiker. Dat gaat ons op dit vlak niet ver genoeg. Liever zien we maatregelen die regeringen en overheden stimuleren om als “launching customer” van innovatieve veiligheidsoplossingen op te treden. Dat stimuleert de particuliere sector om te investeren in innovatieve technologieën, waarmee nieuwe en veiliger oplossingen ontwikkeld kunnen worden.

Smalle scope

Op verschillende terreinen is de strategie niet specifiek genoeg. De EU bevordert grensoverschrijdende publiekprivate samenwerking op het gebied van Critical Information Infrastructure Protection (CIIP) zonder te specificeren op welk niveau. Technisch? Sectorspecifieke certificering? Of ook op tactisch en operationeel niveau? Daarnaast beperkt de focus van de veiligheidsstrategie zich tot internetdiensten en infrastructuur. Dat betekent dat een groot deel van cyberspace (namelijk het deel dat niet rechtstreeks met internet is verbonden) buiten de scope valt. Denk aan mobiele telecommunicatie, procescontrolesystemen, medische apparatuur zoals pacemakers en insulinepompen, digitale televisies, point of sale terminals, ICT in voertuigen, enzovoort. Juist hier is een groot en groeiend beveiligingsrisico aanwezig. Omdat er ook geen Europese definitie van “cyber security” is overeengekomen, zijn interpretatieverschillen denkbaar tussen lidstaten onderling en in de interactie met de EU. Die kunnen de noodzakelijke internationale samenwerking in de weg staan. Voorts is het van belang om de strategie in een continu proces te gieten van risicobeoordeling en integrale PPS-aanpak tot implementatie. De Nederlandse Strategie Nationale Veiligheid (inclusief de Nationale Risicobeoordeling) is daarbij een interessant voorbeeld. Daarnaast is ook de scope van de concept richtlijn te beperkt. Daar ligt de focus op het verzamelen van informatie over incidenten, zonder dat dit gekoppeld is aan een gefundeerde visie op risicomanagement. Dat werkt in de hand dat organisaties verplicht worden irrelevante informatie te verzamelen en te delen, hetgeen de risico-regel-reflex alleen maar versterkt.

Onderwijs en bewustzijn en kennis op directieniveau

In de Europese strategie wordt niet veel aandacht besteed aan het ontwerp en de bevordering van cyber security onderwijs, noch aan het vergroten van kennis en bewustzijn op directieniveau over het cyber risico. De grootste uitdaging is het vergroten van de bewustwording en de risico-management vaardigheden van topmanagers en -ambtenaren. Betrokkenheid van de top bij cyberveiligheid en risicomanagement is van groot belang. Om het hoofd te bieden aan de bestaande en toekomstige behoefte aan cyber security experts en managers met verstand van cyber veiligheid, wordt op initiatief van HSD en gemeente Den Haag gewerkt aan de oprichting van een Cyber Security Academy, die al dit najaar van start gaat.
Experts van Innovatiehuis Cyber Security in The Hague Security Delta hebben de Europese strategie geanalyseerd en schreven binnen enkele dagen na publicatie een reactie. De volledige reactie vindt u op: ww.thehaguesecuritydelta.com/innovation/cybersecurity.